Europäisches Patentamt

European Patent Office

Office européen des brevets

Bescheinigung

Certificate

Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

03014730.0

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 03014730.0
Demande no:

Anmeldetag:
Date of filing: 27.06.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Nokia Corporation
Keilalahdentie 4
02150 Espoo
FINLANDE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Enhanced fast handover procedures

In Anspruch genommene Prioriät(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04Q7/38

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT RO SE SI SK TR LI

TBK TIEDTKE - BÜHLING - KINNE & PARTNER (GbR)

TBK-Patent POB 20 19 18 80019 München

Patentanwälte
Dipl.-Ing. Reinhard Kinne
Dipl.-Ing. Hans-Bernd Pellmann
Dipl.-Ing. Klaus Grams
Dipl.-Ing. Aurel Vollnhals
Dipl.-Ing. Thomas J.A. Leson
Dipl.-Ing. Dr. Georgi Chivarov
Dipl.-Ing. Matthias Grill
Dipl.-Ing. Alexander Kühn
Dipl.-Ing. Rainer Böckelen
Dipl.-Ing. Stefan Klingele
Dipl.-Chem. Stefan Bühling
Dipl.-Ing. Ronald Roth
Dipl.-Ing. Jürgen Faller
Dipl.-Ing. Hans Ludwig Trösch
Rechtsanwälte
Michael Zöbisch

US 38391

June 27, 2003

NOKIA CORPORATION
Espoo, Finland

ENHANCED FAST HANDOVER PROCEDURES

Dresdner Bank	München	Kto. 3939 844	BLZ 700 800 00
Deutsche Bank	München	Kto. 286 1060	BLZ 700 700 10
Postbank	München	Kto. 67043 804	BLZ 700 100 80
Mizuho Corp. Bank	Düsseldorf	Kto. 8104233007	BLZ 300 207 00
UFJ Bank Limited	Düsseldorf	Kto. 500 047	BLZ 301 307 00

/RS218

Telefon: +49 89 544690
Telefax (G3): +49 89 532611
Telefax (G3+G4): +49 89 5329095
E-Mail: postoffice@tbk-patent.de
Internet: http://www.tbk-patent.de
Bavariaring 4-6, 80336 München

TITLE: Enhanced Fast Handover procedures

Field of the invention

This invention relates to a method and a system for handing over a connection of a mobile entity between two network access entities, in case a global address of one or both of the participating network access entities is not known to the mobile entity performing the handover.

Background of the invention

This invention is related to mobile IP networks, and in particular to performing a handover or a movement from one Access Router to another Access Router.

The field of the invention relates to optimised IP-layer handovers (i.e. optimisations to Mobile IPv6) for seamless session mobility. More specifically, the invention is mostly applicable for seamless session continuity during Inter-System handovers or complementary access IP layer handovers (e.g. seamless session continuity between WLAN and 3GPP systems as described in 3GPP TR 22.934 "Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking").

The IETF (Internet Engineering Task Force) is putting significant effort in the standardization of mobile solutions for IP (Internet Protocol) based networks, such as Mobile IP. The solution introduced by these standards may be complemented with other mechanisms, which are being also developed by IETF, in order to enhance the handover performance. For example, the Fast Handover

Internet Draft "draft-ietf-mobileip-fast-mipv6-06.txt", may be used together with Mobile IPv6 to enhance the performance of the IP handover.

Further detailed information concerning Fast Handover can be found in the following documents, for example: "FAST HANDOVERS FOR MOBILE IPv6",EURESCOM Participants in Project P1113 by Sebastien Auvray, France Telecom; "Fast Handovers and Context Transfers in Mobile Networks" by Rajeev Koodli and Charles E. Perkins; and "An Analysis of The Fast Handovers for Mobile IPv6 Protocol" by Janne Lundberg, Helsinki University of Technology, Laboratory for Theoretical Computer Science, May 28, 2003.

These solutions are designed independently of the underlying technology placed below the IP layer. Therefore they could be used for implementing an IP handover between two access technologies as far as both networks, previous access network and target access network, utilize the IP protocol at the network layer. A typical example is mobility across WLAN (Wireless Local Area Network) and GPRS (General Packet Radio Service) networks. Some access technologies (such as GPRS), however, exhibit certain characteristics that may have an impact on the functionality of the IP handover as will be explained in the following.

During a normal session, a Mobile Node (MN) is attached to an Access Router (AR). An Access Router offers IP connectivity to mobile nodes and acts as a default router to the mobile nodes it is currently serving. A serving Access router is also referred to as a SAR (Serving Access Router). The Access Router may include intelligence beyond a simple forwarding service offered by ordinary IP routers. In case the MN wishes to perform

a handover, there are usually some Access Routers to which the MN may do a handover. These Access Routers are referred to as Candidate Access Router (CAR).

The Access Router which is chosen for the handover is referred to as Target Access Router (TAR). In detail, the TAR is the AR with which the procedures for the MN's IP level handover are actually initiated. The TAR is selected after running a TAR selection algorithm that may take into account parameters such as the capabilities of CARs, preference of the MN and any local policies. After the handover, the TAR is then the (new) SAR.

After performing the handover, the old SAR, to which the MN was attached before, is referred to as Previous Access Router (PAR), which is occasionally also referred to as Old Access Router (OAR). The PAR is the (old) SAR that will cease or has ceased to offer connectivity to the MN.

Typically a MN is connected to the AR via an Access Point (AP). An Access Point is a layer 2 device which is connected to one or more Access Routers. Access Points are sometimes called base stations or access point transceivers. An AP may be a separate from AR or co-located with an AR.

In the Fast Handover procedure, a mobile node (MN) sends an F-BU (Fast Binding Update) message when it is about to move to the TAR. Once the PAR has received the F-BU message it starts to forward the incoming packets addressed to MN towards the TAR. The F-BU is the last message sent by the MN before leaving the PAR. Also the MN can send the F-BU message after moving to the TAR (the first message sent after the movement) if it was not possible to send it before the movement took place

The MN always knows the link local IP address of the PAR since the MN can learn this information from the router advertisement messages received from PAR before the movement took place. This information allows the MN to send the F-BU message to the PAR addressed to the PAR's link local IP address whilst the MN is still attached to the PAR's link. However it cannot be assumed that the MN always knows the PAR's publicly routable global unicast IP address and therefore, in the cases the MN does not know the PAR's globally routable IP address, the MN will not be able to send the F-BU message to the PAR after it moves to the target network since it will not able to address the F-BU properly (i.e. to the PAR's globally routable IP address).

This scenario is always present when the MN has to send the F-BU after moving to the target network and the previous access network is GPRS since the globally routable IP address of the GGSN (Gateway GPRS Support Node) is totally unknown for the GPRS UE's (it is assumed that GGSN acts as Access Router for the GPRS network).

The Fast Handover Internet Draft assumes that the MN knows the PAR's globally routable IP address. This does not always apply, for example, when the previous access technology is GPRS (and as a result, the PAR is GGSN). No prior solution is known so far.

The above-mentioned problem, i.e., that the globally routable addresses of Access Routers participating in a handover are not known, has also an effect on other details of the handover procedure.

Several protocols are being designed (in IETF) for seamless IP-level handovers, such as Fast handovers and Context Transfer. Since these protocols constitute IP signalling between the current Access Router (AR) and Target Access Router (TAR), a critical requirement for these mechanisms to work is that the TAR for the Mobile Node's (MN) handover is known to the current AR (Figure 1). The TAR identification problem is being studied in the IETF Seamoby WG (Workgroup) and is subdivided as follows:

- Identification of the neighbouring ARs in advance of handover (HO). This procedure is also known as Candidate Access Router discovery (CAR)

- TAR selection (from the list of CARs) at time of HO

These mechanisms require that the TAR IP address is known for current AR in order to perform a handover. In some situations, this may not be possible/desired for any of the following reasons:

- The TAR resides in a different administrative domain which wants to keep its internal addressing information confidential from other administrative domains.

- The TAR resides in a private IP addressing domain (i.e. the TAR does not have a publicly routable IP address).

- Determination of the TAR requires some access-technology specific procedures.

Hence, in these cases it is not possible to perform a handover to the TAR.

Summary of the invention

Thus, the object underlying the present invention resides in overcoming the above described limitations associated with the access technology characteristics according to the prior art and to enable a handover even in case a global address of one, or both, of the participating network access entities is not known to a mobile entity attempting the handover and/or to another network access entity participating in the handover.

The are two scenarios where the present invention is useful:

1) an IP packet needs to be sent to a previous network access entity whose global IP address is not known neither to the current network access entity, nor to the mobile entity.
2) An IP packet needs to be sent to a target network access entity whose IP address is not known neither to the current network access entity, nor to the mobile entity.

The object, for the first scenario, is solved by a method for handing over a connection of a mobile entity from a first network access entity to a second network access entity, wherein a global address of the first network access entity is not known to the mobile entity, the method comprising the step of

sending a message including information for identifying the first network access entity from the mobile entity to the second network access entity, which enables the second network entity to direct traffic destined to the first network entity.

Alternatively, the above object is solved by a network system comprising at least one mobile entity, a first network access entity and a second network access entity, wherein a global address of the first network access entity is not known to the mobile entity, wherein

the mobile entity is adapted to send a message including information for identifying the first network access entity to the second network access entity which enables the second network entity to direct traffic to the first network entity.

In detail, according to the invention a mechanism is introduced enabling a Mobile Node (MN) as an example for a mobile entity to engage in signaling (e.g., IP signaling) with its off-link previous Access Router (PAR) as an example for the first network access entity, when the publicly routable global unicast IP address of the PAR is not known by the MN. The Mobile Node functionality may be in any mobile station, lap-top computer, PDA equipment or the like.

The delivery of the Fast Binding Update (F-BU) message from MN to PAR in the Fast Handover protocol, when the PAR is a GGSN, is an example when such a mechanism is required. The solution according to this invention applies in the scenarios when the MN has to send the F-BU to the PAR after moving to the target network.

Hence, by using the mechanism proposed by this invention the MN will be able to use the Fast Handover procedure when it performs IP handovers from GPRS to any other target network.

Moreover, the publicly routable global unicast IP address of the GGSN in the GPRS network does not need to be revealed to the MN.

The second network access entity may identify whether the message received from the mobile entity is directed to the first network access entity by checking the address indicated in the message, and check whether the address is globally routable.

On checking the address, it may be judged whether the address is globally routable or not based on a prefix of the address.

The message may be a Fast Binding Update (F-BU) message.

The message including information for identifying the first network access entity may be sent before de-establishing the connection between the mobile entity and the first network entity. Alternatively, the message including information for identifying the first network access entity may be sent after de-establishing the connection between the mobile entity and the first network entity.

When the message including information for identifying the first network access entity is sent before de-establishing the connection between the mobile entity and the first network entity, the second network access entity may receive a message from the first network access entity including the global address of the first network access entity.

The second network access entity may hold a mapping table in which the information for identifying the first

network access entity received from the mobile entity is mapped to a global address of the first network access entity.

The information for identifying the first network access entity may comprise a link layer address of the mobile entity.

Furthermore, a message including all or part of the information for identifying the first network access entity may be sent from the second network access entity to a proxy, wherein the proxy determines the address of the first network access entity.

The information for identifying the first network access entity may comprise at least one of the following parameters:

old network identity (such as, e.g., PLMN ID, Public Land Mobile Network Identity),

old access point name (e.g., GPRS Access Point Name (APN) if the first network access entity was a GGSN),

identity associated with the access point through which the mobile entity was connected to the first network access entity , and/or

a link layer address of the mobile entity.

Hence, the globally routable address of the first network entity is determined by a proxy, so that the global address does not have to be revealed to the second network entity or the mobile entity.

Thus, according to the invention a handover or another kind of change of connection of a mobile entity between two network access entities can be performed even in case the address of one of the participating network access

entities is either not known or is not desired to be publicly known.

The proxy may be also used to forward signalling (and other traffic) between the second network access entity and the first network access entity.

The mobile entity may monitor attributes of the network of the first network access entity, in advance of the handover, in order to obtain information for identifying the first network access entity.

The second network access entity may determine the address of the appropriate proxy based on information included in the information for identifying the first network access entity received from the mobile entity.

Additionally, the above object, for the second scenario, is solved by a method for performing a handing over a connection of a mobile entity from a first network access entity to a second network access entity, wherein a global address of the second network access entity is not known to the mobile entity, the method comprising the step of

sending a message including information for identifying the second network access entity from the mobile entity to the first network access entity, which enables the first network entity to direct traffic to the second network entity.

In addition, the above object is solved by a network system comprising a mobile entity, a first network access entity and a second network access entity, wherein a global address of the second network access entity is not known to the mobile entity, wherein

the mobile entity is adapted to send a message including information for identifying the second network access entity to the first network access entity, which enables the first network entity to direct traffic to the second network entity.

Furthermore, a message including all or part of the information for identifying the second network access entity may be sent to a proxy, wherein the proxy determines the address of the second network access entity.

Hence, the globally routable address of the second network entity is determined by a proxy, so that the global address does not have to be revealed to the first network entity or the mobile entity.

Thus, according to the invention a handover or another kind of change of connection of a mobile entity between two network access entities can be performed even in case the address of one of the participating network access entities is either not known or is not desired to be publicly known.

The proxy may also be used to forward signalling (and other traffic) between the first network access entity and the second network access entity.

The mobile entity may monitor attributes of the network of the second network access entity in order to obtain information for identifying the second network access entity.

The first network access entity may determine the address of the proxy based on information included in the

information for identifying the second network access entity received from the mobile entity.

The first network access entity may identify whether the message received from the mobile entity is directed to the second network access entity by checking the address indicated in the message, and checking whether the address is globally routable.

Furthermore, during checking the address, it may be judged whether the address is globally routable or not based on a prefix of the address.

The message may be a Handover Initiate (HI) message.

The first network access entity may hold a mapping table in which the information for identifying the second network access entity received from the mobile entity is mapped to a global address of the second network access entity.

The information for identifying the second network access entity may comprise at least one of the following parameters:

target network identity (such as, e.g., PLMN ID, Public Land Mobile Network Identity),

target access point name (e.g., target GPRS Access Point Name (APN), if the new connection is a GPRS connection), and/or

identity associated with the access point through which the mobile entity will be connected to the second network access entity.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows a first scenario for a Fast Handover procedure,

Fig. 2 shows a second scenario for a Fast Handover procedure, to which the first embodiment can be applied,

Fig. 3 shows a third scenario for a Fast Handover procedure, to which the first embodiment can be applied,

Fig. 4A and 4B show a general procedure for the solution according to the first embodiment,

Fig. 5 shows a handover signalling between a current Access Router (AR) and a Target Access Router (TAR) according to the prior art,

Fig. 6 illustrates TAR IP address discovery according to a simple example according to the second embodiment,

Fig. 7 illustrates TAR IP address discovery based on a proxy function in the target network according to the second embodiment,

Fig. 8 shows a signalling flow of the TAR IP address discovery based on the proxy function in the target network according to the second embodiment

Fig. 9 shows details of step S5 of the signalling flow of Fig. 8,

Fig. 10 shows security associations required when using a solution without the proxy according to the second embodiment,

Fig. 11 shows security associations required when using the proxy according to the second embodiment, and

Fig. 12 shows a combination of the first and the second embodiment according to which a proxy is used to determine the global address of the PAR.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

In the following, preferred embodiments are described by referring to the enclosed drawings.

According to a first embodiment, a change of connection (i.e., a handover or a movement) of a mobile entity from a first network access entity to a second network access entity is performed such that the mobile entity sends a message including information for identifying the first network access entity to the second network which enables the second network entity to acquire a global address of the first network entity. That is, in case the global address of the first network access entity is necessary to accomplish the handover and the mobile entity (e.g., Mobile IPv6 Mobile Node MN) does not know it, the mobile entity sends known information associated with the first network access entity known to the second network entity. By using this information, the second network entity is capable to acquire the global address of the first network access entity, such that the handover or movement procedure can be completed.

It is noted that in the context of this application the term "global address" refers to an address that has significance in the TAR (Target Access Router as an example for the second network entity) network (i.e. an

address that can be used to reach the PAR (Previous Access Router as an example for the first network entity) from the TAR). That is, a "global address" refers to an address, which is generally known (or available) in the network. In contrast thereto, the term "local address" refers to an address which is only available locally, i.e., only in a part of the network. For example, in the present case the link local address of the first network access entity (e.g., PAR) may be used only is the mobile entity resides on the same link.

The above procedure is described in the following in more detail.

Fig. 1, Fig. 2 and Fig. 3 show different scenarios for the Fast Handover procedure mentioned in the introductory part.

In these scenarios, it is assumed that a Mobile node (MN) moves from a Previous Access Router (PAR) as an example for a first network access entity to a Target Access Router (TAR) as an example for a second network access entity. It is assumed that the PAR is located in a Subnet 1 - Access Network 1, and the TAR is located in a Subnet 2 - Access Network 2.

It is noted that the figures do not show all the elements involved in the signalling. For example, the APs are located in between the Access Routers and mobile nodes.

Fig. 1 illustrates a scenario of a so-called scenario for an "Anticipated case". That is, here, a Fast Handover procedure is initiated before the movement.

The handover is initiated by the MN by sending a Router Solicitation message for proxy (RtrSolPr) to the PAR in message 11. This is a message from the MN to the PAR requesting information for a potential handover. The PAR sends a Handover Initiate message (message 12) to the TAR. As a response to the HI message, the TAR sends a HACK (Handover Acknowledgement) message to the PAR (message 13). After receiving the HACK message from the TAR, the PAR sends a Proxy Router Advertisement message to the MN (message 14). The Proxy Router Advertisement (PrRtAdv) is a message from the PAR indicating a MN to undergo the handover.

Thereafter, the MN sends a Fast Binding Update (F-BU) message 15 to the PAR. The Fast Binding Update (F-BU) message is a message from the MN instructing its PAR to redirect its traffic towards NAR, i.e., TAR. Thus, this message is important to complete the handover.

After the movement, the MN sends a Fast Neighbor Advertisement message to the TAR. The Fast Neighbor Advertisement (FNA) is a message from the MN to the NAR (here TAR) to confirm use of NCoA (New Care of Address) when the MN has not received Fast Binding Acknowledgement (FBACK). Namely, in the present case the PAR has not sent a FBACK message to the MN because it has just moved to the TAR. In response to the FNA message 16, the TAR sends a FBACK message (message 17) to the MN. By this message, the Fast Handover procedure is completed.

It is noted that Care of Address (CoA) is a temporary address allocated for the MN while it is visiting foreign networks. Home Agent maintains a binding between the static Home address of the MN and the current CoA.

Hence, in scenario 1 shown in Fig. 1 the MN sends the F-BU message 15 whilst it is still attached to the previous access network. The MN thus does not have any problem when sending the F-BU message to PAR since it is located in the same link as the PAR. The MN uses the PAR's link local IP address to address the F-BU to PAR.

In Fig. 2, a scenario 2 is illustrated. The messages 21 to 24 correspond to the messages 11 to 14 shown in Fig. 1. However, here the MN sends the F-BU message (message 25) after it has moved to the TAR. This message, however, must be directed to the PAR, since the PAR has to be requested to redirect the traffic of the MN (packets addressed to the old CoA of the MN) to the TAR. Thus, the TAR has to forward the F-BU message to the PAR in message 25. In the case the MN does not know the PAR's globally routable IP address the MN cannot be able to address the F-BU message properly to PAR unless the solution according to the present embodiment of the invention is used.

Namely, as will be explained later in detail, the information which the MN additionally inserts into the F-BU message is used in order to determine the globally routable IP address of the PAR.

After sending the F-BU message 25, the MN sends a FNA message (message 26) to the TAR, which responds with a FBACK message (message 27) in order to complete the Fast Handover procedure.

It is noted that the FNA is sent after the MN reaches the new access network. It is used to start the delivery of buffered packets from TAR to MN. FBU starts the forwarding of packets from PAR to TAR. At this point the

TAR buffers the packets until the MN arrives to the new access network. When the MN reaches the TAR, the sending of FNA starts the delivery of those buffered packets from TAR to MN.

Fig. 3 illustrates a scenario for a so-called "Non-Anticipated case", i.e., the Fast Handover procedure is initiated after the movement.

That is, in this case the Fast Handover procedure starts by sending a F-BU message (message 31) from the MN to the TAR. This F-BU message has to be forwarded to the PAR, similar to the case shown in Fig. 2. After this, the PAR sends a HI message (message 32) to the TAR, and the TAR responds with a HACK message (message 33). Thereafter, the TAR sends a FBACK message (message 34) to the MN to complete the Fast Handover procedure.

Thus, in scenario 3 the MN starts the Fast Handover procedure by sending a F-BU message after the movement. In the case the MN does not know the PAR's globally routable IP address the MN cannot be able to address the F-BU message properly to PAR unless the solution according to the present embodiment of the invention is used.

Figs. 4A and 4B illustrates the general procedure for the solution described in this invention.

As a general requirement, in the "Anticipated case" of the Fast Handover procedure, the so-called MN_LLA (which carries the MN's link-layer identity, such as MAC address) option must be included in all the RtrSolPr, HI and F-BU messages of the Fast Handover procedure. This will enable the TAR to map the MN_LLA with the PAR's

publicly routable global unicast address as described below.

MN-LLA is the Link-layer address of MN, and is in particular the link-layer address of the MN that is undergoing handover to the destination. According to the above referenced Fast Handover Internet Draft ("draft-ietf-mobileip-fast-mipv6-06.txt"), this option should be included to help the destination recognize the MN when it connects to the destination.

Figs. 4A and 4B illustrate the proposed procedure step by step:

1. Two possible scenarios, "anticipated case" and "non-anticipated case" (as described in Fig. 2 and Fig. 3) are considered:

a) "Anticipated Handover" case (Fig. 4A): when the TAR receives a HI message, the TAR maps the source IP address of the packet (PAR's publicly routable global unicast IP address, which is reachable from the TAR) with the MN_LLA included in that message. This a new feature according to the present embodiment for an AR implementing the Fast Handover functionality.

b) "Non-anticipated handover" case (Fig. 4B): as described above with respect to Fig. 3, in case the F-BU message was not sent before the movement, the MN sends the F-BU message to the PAR after the movement. This message is addressed to the PAR at IP level but the Layer 2 (L2) frame is targeted to the TAR interface (next step in the routing path). The MN includes the following information in the message:

- Destination Address (D.A.): the link local address of the PAR (as specified in the above referenced Fast Handover draft)
- Source Address (S.A.): the MN_PCoA, i.e., the Previous Care of Address of the Mobile Node (as specified in the above referenced Fast Handover draft)

At this point the NAR cannot forward the F-BU message to the PAR since the link local address is not globally routable and the NAR does not know the PAR's public IP address neither.

Thus, according to the present embodiment, some new parameters are proposed to be included in the F-BU message (labelled as optional since they are only useful for the case where the MN sends the F-BU after the movement ("non-anticipated handover" case)) whose goal is to enable the TAR to forward the F-BU message to the correct PAR:

- Old NET_ID: Network identity of the previous access network.
- Old APN_name | old AP_name: name of (GPRS) APN (Access Point Name) or (WLAN) AP (Access Point) which the MN was connected to in the previous access network.
- MN_LLA: link layer address of the MN.

For example, the old network identity may be a PLMN ID (Public Land Mobile Network identity).

2. After receiving the F-BU the TAR checks the D.A. of the packet. It realizes that the target IP address is a link local IP address (characterized by a prefix of FE80)

which is not belonging to itself. The TAR thus checks whether there is an entry for the MN_LLA, which is included by the MN in the F-BU, in the mapping table created by mapping the PAR's publicly routable global IP address with the MN_LLA (information received into the HI message, as described in step 1.a), above):

a) In case there is an entry for the MN_LLA (i.e. HI message was already received by TAR) and the PAR has revealed it´s IP address, then the TAR obtains the PAR's IP address associated and forwards the F-BU message directly to the PAR (IP encapsulation can be used for the forwarding). This would apply for scenario 2 (anticipated case).

b) In case there is not any entry for the MN_LLA, then the TAR forwards the F-BU message to the PAR, whose publicly routable global unicast address is determined with the help of the "old NET_ID" and "APN_name | old AP_name" options included by the MN in the F-BU message. The NAR may need the assistance of a node acting as a proxy in order to be able to perform this mapping which is described later by referring to a second embodiment of the present invention. After the publicly routable global unicast IP address of the PAR is determined, the F-BU message can be forwarded to the PAR (e.g. Via IP-in-IP encapsulation). This would apply for scenario 3 (non-anticipated case).

As a modification of the first embodiment, a situation can be handled in which the globally routable address of the TAR is not know to the MN. That is, in this modification, the roles of the PAR and the TAR with respect to determining a globally routable address are exchanged.

The address of the TAR can be determined basically in the same way as according to the first embodiment.

When, the mapping according to the first embodiment is applied, the PAR holds a mapping table in which the information for identifying the TAR received from the MN is mapped to a global address of the TAR.

In the following, a second embodiment of the invention is described. The second embodiment is directed to TAR identification.

As mentioned in the introductory part, the TAR identification mechanism requires that the current AR determines the IP address of the TAR for the MN's handover. This is illustrated in Fig. 5, for example. Fig. 5 depicts the basic interaction at IP layer between the current AR and the TAR. That is, the IP handover signalling between the current AR and the TAR requires that the current AR knows the target AR globally routable (public) IP address. It is noted that also TAR needs the address of PAR.

Fig. 6 shows a high level schematic of the TAR IP address discovery. In particular, a situation is illustrated in which the globally routable (public) IP address of the TAR is not known to the MN. A mobile node MN is attached to a current AR and wishes to perform a handover to a TAR (target AR). In Fig. 6 it is illustrated that the corresponding access points are Layer 2 Access Points (e.g. WLAN AP's). According to this example, a similar procedure as according to the first embodiment is adopted. Namely, the MN delivers information to the corresponding AR in order to identify the other AR (in

this case, the TAR). In particular, in step S61, the MN monitors attributes (e.g., target WLAN AP MAC address) from the target network point of attachment which will help to identify the TAR IP address. In step S62, the attributes are reported to the current AR. In step S63, the current AR determines the IP address of TAR based on the attributes passed by the MN. Thus, in step S64, the current AR can send the IP handover signalling to the correct TAR.

It is noted that step S63 requires that the AR has access to a mapping table which maps Layer 2 IDs to (e.g. WLAN AP MAC addresses) to the corresponding AR IP address. However, this will not work for GPRS, since a given cell ID will not always map to the same GGSN - depending on what Access Point Name (APN) the MN is going to access. In GPRS the APN is a logical name describing the actual connected access point to the external packet data network according to DNS naming conventions. It refers to the GGSN to be used.

As mentioned above, this requires that the current AR knows the globally routable IP address of the TAR. In some situations, however, this may not be possible/desired for any the following reasons:

- The TAR resides in a different administrative domain which wants to keep its internal addressing information confidential from other administrative domains. For example when a MN is moving from WLAN to GPRS, the TAR will be a GGSN in the GPRS network. If the WLAN is not administered by the GPRS operator (for example WLAN is administered by a University and the GPRS is administered by an Operator X), the GPRS operator (Operator X) is most likely unwilling to reveal its internal addressing (GGSN

IP address) to the WLAN operator (University). Such information could be used, for example, to mount Denial of Service (DoS) attacks on the GGSN. In addition GGSN addressing information may be considered as confidential information by the GPRS operator.

- The TAR resides in a private IP addressing domain (i.e. the TAR does not have a publicly routable IP address). Another possibility is that the TAR does not have a globally routable IP address. This IP address, thus, cannot be used by the current AR for addressing the TAR (unless the current AR and TAR reside in the same private IP addressing space).

- Determination of the TAR requires some access-technology specific procedures.

In addition to the above, there exist additional problems which are solved according to the second embodiment. The following may be considered as the most important problems:

- In Inter system handover WLAN to GPRS, the MN's target GGSN (TAR) will depend on the APN which the MN will access. As a result, the Layer 2 Access Point Identifier to TAR IP address mapping mechanism, will not work. Since in GPRS, the target GGSN depends on APN, the WLAN AR would need to be aware of APN-to-GGSN mappings which are typically maintained in a Domain Name Server (DNS) server in the GPRS operator's network.

- In some Access Networks, determination of the TAR IP address requires some access-network specific functions. It is highly undesirable to expose these functions to other access networks. For example, determining the TAR

in GPRS means identifying the IP address of the target GGSN. In GPRS the target GGSN depends on the APN that the MN wants to access. The GPRS to APN mapping determined by the Serving GPRS Support Node (SGSN) by performing a DNS query. Once again, if the WLAN is not administered by the GPRS operator, the GPRS operator is highly unlikely to be willing to allow the WLAN operator to perform DNS query on its internal nodes. In addition it would be desirable to maintain the GPRS specific details transparent from the WLAN network. It would be, thus, beneficial if the WLAN operator would not need to perform any GPRS specific operations in order to determine the target GGSN IP address.

According to the second embodiment of the invention, a proxy function between administrative domains is introduced in order to allow the current AR to perform the required IP signalling towards the TAR (e.g. Fast Handover or Context Transfer signalling) without revealing the IP address of the TAR to the current AR (Fig. 6). In addition to this, the proxy function hides whatever access-network specific procedures are required in order to determine the TAR IP address. As a result, all target access networks will look the same from the current Access Router point of view. All the access specific functions are performed by the proxy residing in the specific access network. This is shown in Fig. 7:

The MN delivers an information container containing access specific attributes about the target access network (step S72). For this, the MN monitors the attributes from the target network point of attachment which will help to identify the TAR IP address (e.g., target network PLMN ID) in step S71.

The current Access Router uses some of these attributes to identify the target access network and corresponding proxy, and passes the rest of the attributes transparently to the identified proxy. In detail, in step S73 the current AR determines the IP address of the target network proxy corresponding to the attribute parameters passed by the MN (e.g., PLMN ID), and in step S74 IP handover signalling takes place between the current AR and the proxy.

The proxy then performs all the target access network specific procedures required for determining the target Access Router IP address. The same node may also additionally proxy all the IP signalling between the current and target Access Routers, that is, the target Access Router IP address is not revealed to the current Access Router, which may be administered by a different operator, nor to the MN. From the current Access Router's point of view, everything will appear as if it was communicating directly with the target Access Router, or more specifically, with a target Access Router which resides in the same access technology.

In detail, in step S75, the proxy performs access network specific function required for mapping the TAR IP address. In the GPRS case this means a DNS (Domain Name Server) query based on APN. Then, in step S76, the proxy proxies the IP HO (Handover) signalling between the current AR and the TAR (which is, in the GPRS case, a GGSN).

Thus, as illustrated in Fig. 7, the proxy entity performs all the access specific functions required for determining the TAR IP address. The proxy also hides the GPRS internal addressing from the WLAN network entities.

The procedure according to the present embodiment of the invention will be described in the following in more detail with reference to a specific scenario of WLAN to GPRS handover, as illustrated in Fig. 8. Fig. 8 shows signalling flow of TAR IP address discovery based on proxy function in target network. It is noted that the messages "RtrSolPr" (Router Solicitation for Proxy), "HI" (Handover Initiate) and "HACK" (Handover Acknowledgement) are also described in the first embodiment, and are also described in Fast Handovers for Mobile IPv6 "draft-ietf-mobileip-fast-mipv6-06.txt", for example.

As a pre-requisite to the following steps, the current AR needs to have access to a table "T" which maps the identities of potential target networks (e.g. PLMN IDs) to the IP address of the corresponding proxy (e.g. for signalling to Operator Y use proxy IP address Z)

In step S1, the MN gathers attributes "A" useful in identifying target network point of attachment (e.g., PLMN ID + APN). That is, the MN determines information about its target network point of attachment, by monitoring broadcast channels (also known as beacon in cellular systems) for example. The level of information that the MN can determine depends on the terminal capabilities and the type of target access network.

In step S2, the MN sends the identified parameters about target GGSN to the current AR (i.e. the WLAN AR). These can be embedded in the RtrSolPr message in Fast Handovers, for example. The MN may need to include additional parameters required for identifying the TAR. In the GPRS case the MN would need to report the Access Point Name (APN) that the MN's applications will require

when using GPRS access, for example. In particular in the RtrSolPr message, an additional RtrSolPr Option or a new Destination Option containing the attributes "A" gathered in step S1 could be added.

In step S3, the current AR (in this example, the WLAN AR) determines target GPRS network (from the parameters passed by the MN) and identifies the address of the corresponding proxy from a list of available proxies (the WLAN network operator maintains a list of potential target networks and corresponding proxies in a table "T", as described above). That is, the WLAN AR uses some attributes "A" (e.g., PLMN ID) to determine target network and corresponding proxy.

In step S4, the MN sends the message intended for the GGSN (e.g., HI message in fast handovers) to the IP address of the identified proxy in step 3. This message contains a destination option including the parameters which can be used to identify the target GGSN (these parameters are the same ones passed by the MN in step S2). That is, the MN sends a HI message + new Destination Option containing attributes "A" copied from the RtrSolPr message in step S2.

In step S5, the proxy extracts the information from the destination option and determines the GGSN IP address corresponding to the parameters passed by the WLAN AR. For the specific case of WLAN to GPRS handover, this could be done by performing a DNS query in the GPRS network, based on the APN contained in the message received by the proxy. This is illustrated in Fig. 7 by step S75.

In addition, this is also illustrated in Fig. 9, which illustrates step S5 in Fig. 8 in more detail for the case in which the target network is using DNS for solving the address of the Target Access Router. Namely, in step S5a, the proxy sends a DNS query for APN to a DNS. In case the DNS successfully determines the IP address, it sends a DNS response containing the TAR IP address in step S5b to the proxy.

In step S6 the proxy forwards the message received from the WLAN AR (excluding the destination option) to the identified GGSN. This message needs to include a new ID option which helps the proxy identify to which WLAN AR it should send the corresponding response. In order to allow this, the AR also needs to maintain a temporary state which maps the WLAN AR IP address (read from the source address of the incoming packet) to the message ID used in the message forwarded to the GGSN. Alternatively, the message ID could be = WLAN AR IP address, in which case the proxy does not need to maintain any state. Hence, in step S6, the proxy sends a HI message (without the Destination Option containing the attributes) + new Destination option containing the IP address of the current AR, which was extracted from the IP header of the message sent in step S4.

In step S7, the TAR (in this case, the GGSN) receives the message, and performs the necessary actions. The GGSN sends the reply message to the proxy. The message must include a copy of the message ID option, in order to help the proxy identify to which WLAN AR to forward the message. That is, the GGSN sends a HACK message + Destination option containing the IP address of the current AR, which was copied from the message sent in step S6.

In step S8, the proxy receives the response message, strips off the message ID option and uses it to determine the target WLAN AR which the response should be forwarded to. The proxy then forwards the response message to the intended WLAN AR which sent the request message. That is, in step S8, the proxy sends a HACK message (without the Destination Option), and the proxy determines the destination IP address from the Destination Option in the message sent in step S7.

In the following, the effects of the second embodiment with respect to the security associations required are described.

Fig. 10 shows security associations required for the "standard solution", in case no proxy as according to the second embodiment would be used.

In general, IP mobility signalling between Access Routers requires a Security Association between the Access Routers so that the IP mobility signalling can be protected. Fig. 10 illustrates that for the "standard solutions" n^2 Security Associations are required for n geographically adjacent Access Routers. In the example shown in Fig. 10, 3 WLAN Access Routers (indicated in Fig. 10 by WLAN AR #1 to WLAN AR # 3) bordering a region covered by 3 GGSNs (indicated in Fig. 10 by GGSN #1 to GGSN #3) leads to a requirement of $3^2 = 9$ Security Associations (indicated in Fig. 10 by SA #1 to SA #9). This leads to an exponential complexity.

Figure 11 illustrates security associations required for the solution according to the second embodiment.

According to the second embodiment, a Security Association is only required between the proxy and each Access Router. This leads n Security Associations required for n geographically adjacent Access Routers, which corresponds to a linear complexity. In the example of Fig. 11, again 3 WLAN Access Routers and 3 GGSN are shown. Here, only 6 Security Associations are required.

As a modification of the second embodiment, also here the reversed case can be applied, similar to the modification of the first embodiment.

The invention is not limited to the embodiments described above but can vary within the scope of the claims.

For example, the above embodiments can be freely combined.

In particular, the proxy function described in the second embodiment can be used for the procedure according to the first embodiment and according to the modification of the first embodiment.

Namely, in case there is not any entry for the MN_LLA in the procedure according to the first embodiment as illustrated in Fig. 3, for example, the TAR forwards the F-BU message to the PAR, whose publicly routable global unicast address is determined with the help of the "old NET_ID" and "APN_name | old AP_name" options included by the MN in the F-BU message. In this case, the NAR may need the assistance of a node acting as a proxy in order to be able to perform this mapping. This node can be the proxy as described in the second embodiment.

Fig. 12 illustrates this case. Here, a similar situation as in Fig. 3 is shown (Scenario 3), wherein, however, a proxy is used. In message 121 the F-BU message including the parameters described in the first embodiment is sent from the MN to the TAR. In contrast to the first embodiment, the TAR does not try to find out the globally routable IP address of the PAR but forwards the F-BU message to the proxy. Now, the proxy determines the globally routable IP address of the PAR, if necessary, with the help of a DNS query. After obtaining the address, the proxy forwards the F-BU message to the PAR.

After this, also the HI message (message 122) is forwarded to the TAR via the proxy, and also the HACK message (message 123) is sent from the TAR to the PAR via the proxy. That is, it is not necessary that the globally routable IP address of the PAR is known to the TAR or the MN. In order to complete the handover procedure, the FBACK message is sent to the MN in message 124, similar to message 34 in Fig. 3, for example.

Moreover, the invention and in particular the second embodiment focuses on the proxy implementation for WLAN to GPRS interworking. However, the invention is not limited thereon. The same principle could be used between other access technologies, or even inside the same access technology, when IP mobility signalling between different administrative domains is required without revealing any confidential addressing, and without requiring access specific procedures, from the target access network to the current access network.

The details given in the description of the first and the second embodiment and the modifications thereof indicate that all the required options are "piggybacked" (i.e.,

carried) on already existing signalling messages (namely Fast Handover messages). The information contained in these options could be equally transmitted through other mechanisms such as Internet Control Message Protocol (ICMP) options, for example.

The details of the internal functions of the proxy, as described in the first and second embodiment and the modifications thereof were specific to GPRS. This does not limit the applicability of this invention to WLAN to GPRS handovers, however. If the target network is WLAN, for example, the proxy could maintain a table which maps the relevant WLAN AP MAC addresses to the corresponding AR IP address.

The mobile node (MN)as an example for a mobile entity mentioned in the above described embodiments is only an example for a general network element. That is, the invention is applicable to any entity which can perform a handover or change of connection between two network access entities.

In particular, in this application the term "mobile entity" is used to refer to any entity which switches its IP connectivity from one network access entity to another network access entity. This changeover may be caused by, but not limited to, for example, mobility of the mobile entity, selection by the end user of the mobile entity, or a trigger coming from the network end.

CLAIMS

1. A method for handing over a connection of a mobile entity from a first network access entity to a second network access entity, wherein a global address of the first network access entity is not known to the mobile entity, the method comprising the step of

sending a message including information for identifying the first network access entity from the mobile entity to the second network access entity, which enables the second network entity to direct traffic destined to the first network entity.

2. The method according to claim 1, further comprising the step of identifying, in the second network access entity, whether the message received from the mobile entity is directed to the first network access entity by checking the address indicated in the message, and checking whether the address is globally routable.

3. The method according to claim 2, wherein in the address checking step, it is judged whether the address is globally routable or not based on a prefix of the address.

4. The method according to claim 1 or 2, wherein the message is a Fast Binding Update (F-BU) message.

5. The method according to claim 1, wherein the message including information for identifying the first network access entity is sent before de-establishing the connection between the mobile entity and the first network entity.

6. The method according to claim 1, wherein the message including information for identifying the first network access entity is sent after de-establishing the connection between the mobile entity and the first network entity.

7. The method according to claim 1, wherein

the second network access entity receives a message (22) from the first network access entity including the global address of the first network access entity.

8. The method according to claim 1 or 7, wherein

the second network access entity holds a mapping table in which the information for identifying the first network access entity received from the mobile entity is mapped to a global address of the first network access entity.

9. The method according to claim 1, wherein the information for identifying the first network access entity comprises at least one of the following parameters:

a old network identity associated with the first network access entity,

old access point name,

identity associated with the access point through which the mobile entity was connected to the first network access entity , and/or

a link layer address of the mobile entity.

10. The method according to claim 1, further comprising the step of

sending a message including all or part of the information for identifying the first network access entity to a proxy, wherein

the proxy determines the address of the first network access entity.

11. The method according to claim 10, wherein the proxy forwards traffic between the second network access entity and the first network access entity.

12. The method according to claim 1, wherein the mobile entity monitors attributes of the network of the first network access entity in order to obtain information for identifying the first network access entity.

13. The method according to claim 10, wherein the second network access entity determines the address of the proxy based on information included in the information for identifying the first network access entity received from the mobile entity.

14. A method for performing a handing over a connection of a mobile entity from a first network access entity to a second network access entity, wherein a global address of the second network access entity is not known to the mobile entity, the method comprising the steps of

sending (S72) a message including information for identifying the second network access entity from the mobile entity to the first network access entity, which enables the first network entity to direct traffic to the second network entity.

15. The method according to claim 14, further comprising the step of

sending (S74), a message including all or part of the information for identifying the second network access entity to a proxy, wherein

the proxy determines the address of the second network access entity.

16. The method according to claim 15, wherein the proxy forwards traffic between the first network access entity and the second network access entity.

17. The method according to claim 14, wherein the mobile entity monitors attributes of the network of the second network access entity in order to obtain information for identifying the second network access entity.

18. The method according to claim 15, wherein the first network access entity determines the address of the proxy based on information included in the information for identifying the second network access entity received from the mobile entity.

19. The method according to claim 14, further comprising the step of identifying, in the first network access entity, whether the message received from the mobile entity is directed to the second network access entity by checking the address indicated in the message, and checking whether the address is globally routable.

20. The method according to claim 19, wherein in the address checking step, it is judged whether the address is globally routable or not based on a prefix of the address.

21. The method according to claim 14 or 19, wherein the message is a handover Initiate (HI) message.

22. The method according to claim 14, wherein

the first network access entity holds a mapping table in which the information for identifying the second network access entity received from the mobile entity is mapped to a global address of the second network access entity.

23. The method according to claim 14, wherein the information for identifying the second network access entity comprises at least one of the following parameters:

a target network identity,

a target access point name,

identity associated with the access point through which the mobile entity will be connected to the second network access entity.

24. A network system comprising at least one mobile entity, a first network access entity and a second network access entity, wherein a global address of the first network access entity is not known to the mobile entity, wherein

the mobile entity is adapted to send a message including information for identifying the first network access entity to the second network access entity which enables the second network entity to direct traffic to the first network entity.

25. The network system according to claim 24, wherein

the second network access entity is adapted to identify whether the message received from the mobile entity is directed to the first network access entity by checking the address indicated in the message, and to check whether the address is globally routable.

26. The network system according to claim 24 or 25, wherein the message is a Fast Binding Update (F-BU) message.

27. The network system according to claim 24, wherein

the second network access entity is adapted to hold a mapping table in which the information for identifying the first network access entity received from the mobile entity is mapped to a global address of the first network access entity.

28. The network system according to claim 24, wherein the information for identifying the first network access entity comprises at least one of the following parameters:

old network identity associated with the first network access entity,

old access point name,

identity associated with the access point through which the mobile entity was connected to the first network access entity, and/or

a link layer address of the mobile entity.

29. The network system according to claim 24, wherein

the first network access entity is adapted to send a message including all or part of the information for identifying the second network access entity to a proxy, and

the proxy is adapted to determine the address of the second network access entity.

30. The network system according to claim 29, wherein the proxy is adapted to forward traffic between the first network access entity and the second network access entity.

31. The network system according to claim 24, wherein the mobile entity is adapted to monitor attributes of the network of the second network access entity in order to obtain information for identifying the second network access entity.

32. The network system according to claim 29, wherein the second network access entity is adapted to determine the address of the proxy based on information included in the information for identifying the first network access entity received from the mobile entity.

33. A network system comprising a mobile entity, a first network access entity and a second network access entity, wherein a global address of the second network access entity is not known to the mobile entity, wherein

the mobile entity is adapted to send a message including information for identifying the second network access entity to the first network access entity, which enables the first network entity to direct traffic to the second network entity.

34. The network system according to claim 33, wherein

the first network access entity is adapted to send a message including all or part of the information for identifying the second network access entity to a proxy, and

the proxy is adapted to determine the address of the second network access entity.

35. The network system according to claim 34, wherein the proxy is adapted to forward traffic between the first network access entity and the second network access entity.

36. The network system according to claim 33, wherein the mobile entity is adapted to monitor attributes of the network of the second network access entity in order to obtain information for identifying the second network access entity.

37. The network system according to claim 34, wherein the first network access entity is adapted to determine the address of the proxy based on information included in the information for identifying the second network access entity received from the mobile entity.

38. The network system according to claim 33, wherein the message is a handover Initiate (HI) message.

39. The network system according to claim 33, wherein the first network access entity is adapted to hold a mapping table in which the information for identifying the second network access entity received from the mobile entity is mapped to a global address of the second network access entity.

40. The network system according to claim 33, wherein the information for identifying the second network access entity comprises at least one of the following parameters:

a target network identity,

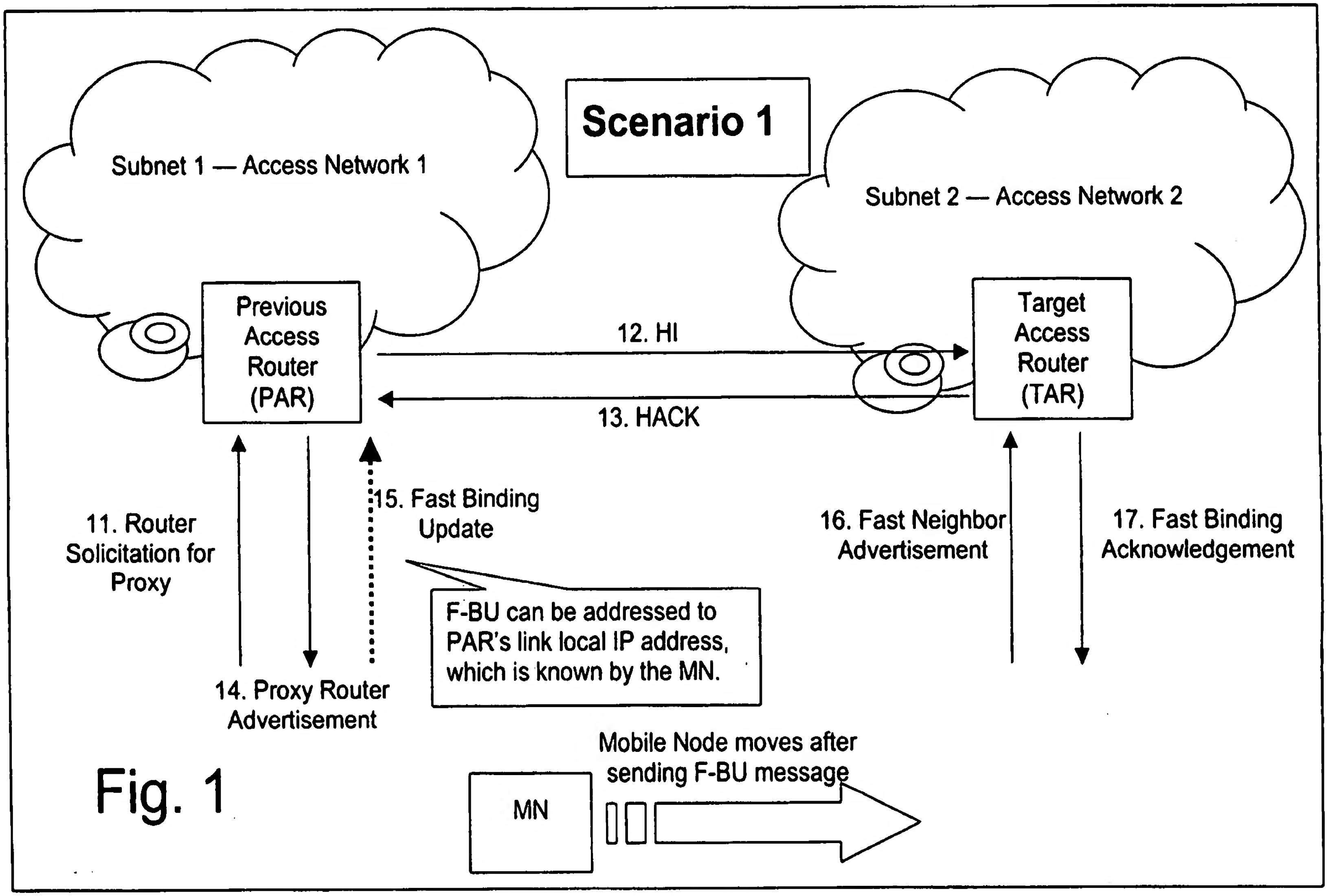
target access point name,

identity associated with the access point through which the mobile entity will be connected to the second network access entity.

ABSTRACT

The invention proposes a method for performing a change of a connection of a mobile entity from a first network access entity to a second network access entity, wherein a global address of the first network access entity is not known to the mobile entity, the method comprising the step of sending a message including information for identifying the first network access entity from the mobile entity to the second network access entity which enables the second network entity to direct traffic to the first network entity. The invention also proposes a method for the reverse direction, i.e. for sending IP signalling from the mobile entity or from the first network access entity towards the second network access entity, whose global IP address is not known by the mobile entity or first network access entity.

(Fig. 3)



Scenario 1
Subnet 1 — Access Network 1
Subnet 2 — Access Network 2
Previous Access Router (PAR)
Target Access Router (TAR)
12. HI
13. HACK
11. Router Solicitation for Proxy
14. Proxy Router Advertisement
15. Fast Binding Update
F-BU can be addressed to PAR's link local IP address, which is known by the MN.
16. Fast Neighbor Advertisement
17. Fast Binding Acknowledgement
Mobile Node moves after sending F-BU message
MN

Fig. 1

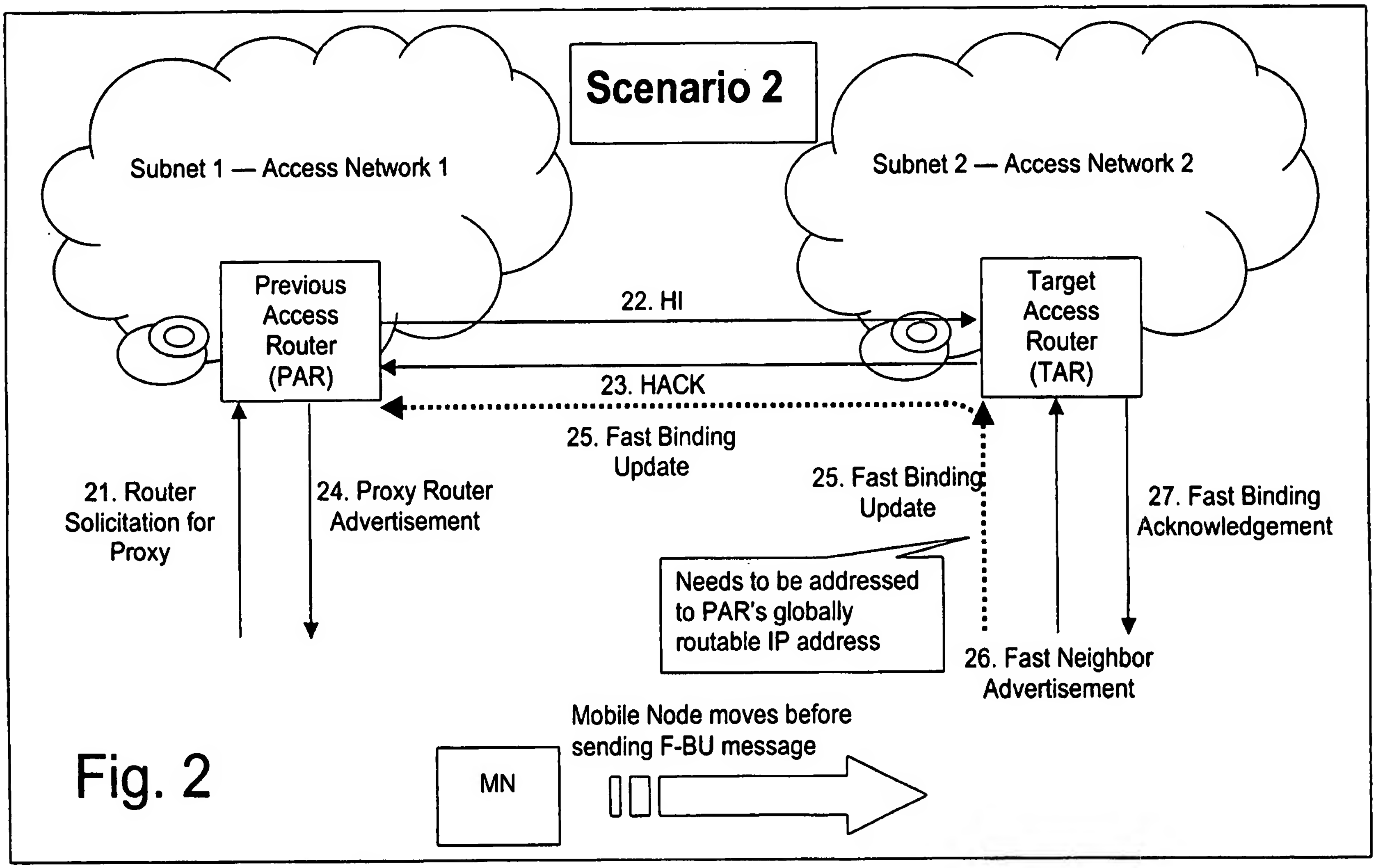

Scenario 2
Subnet 1 — Access Network 1
Subnet 2 — Access Network 2
Previous Access Router (PAR)
Target Access Router (TAR)
22. HI
23. HACK
25. Fast Binding Update
25. Fast Binding Update
21. Router Solicitation for Proxy
24. Proxy Router Advertisement
Needs to be addressed to PAR's globally routable IP address
26. Fast Neighbor Advertisement
27. Fast Binding Acknowledgement
Mobile Node moves before sending F-BU message
MN

Fig. 2

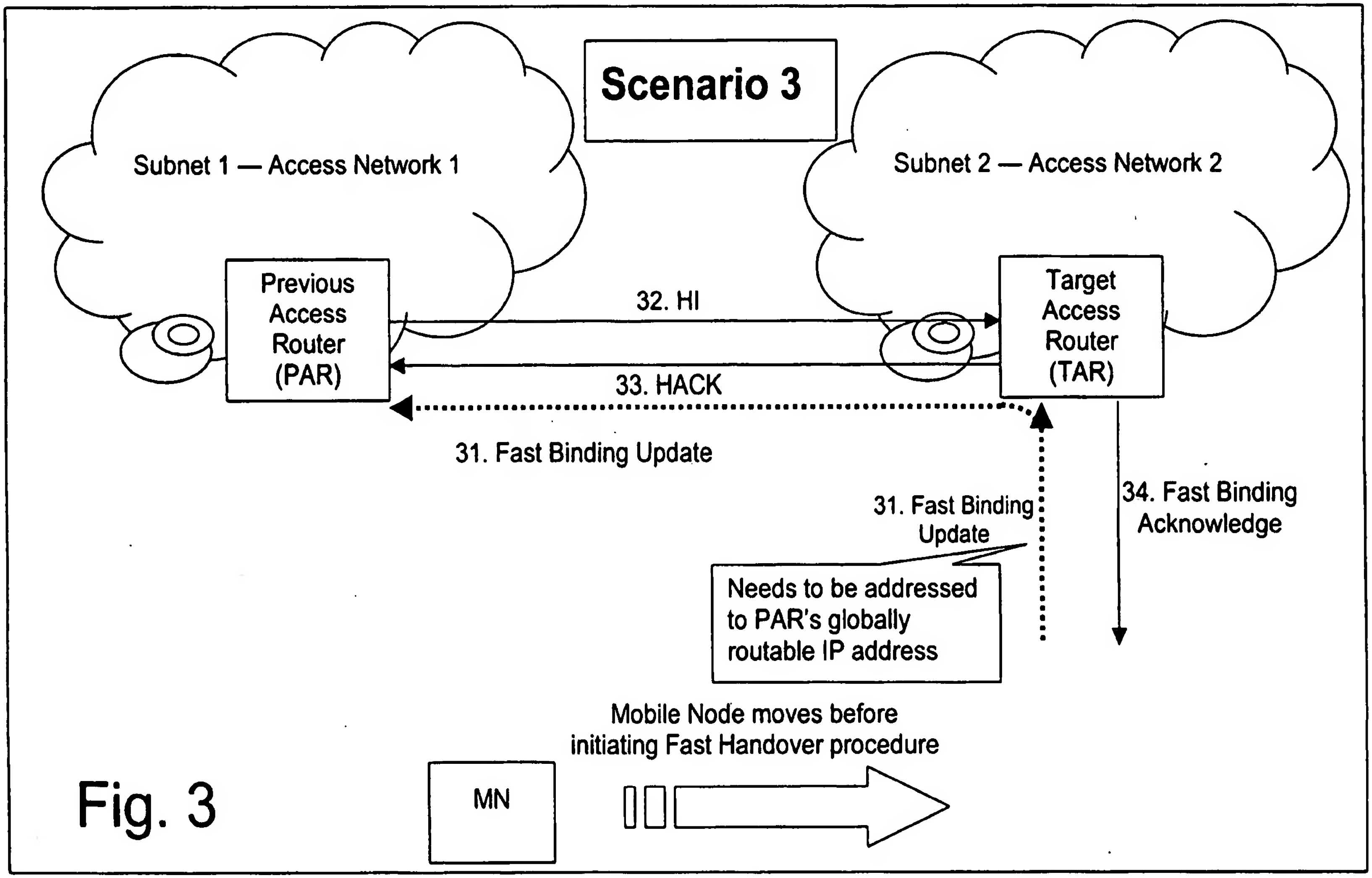

Scenario 3
Subnet 1 — Access Network 1
Subnet 2 — Access Network 2
Previous Access Router (PAR)
Target Access Router (TAR)
32. HI
33. HACK
31. Fast Binding Update
31. Fast Binding Update
Needs to be addressed to PAR's globally routable IP address
34. Fast Binding Acknowledge
Mobile Node moves before initiating Fast Handover procedure
MN

Fig. 3

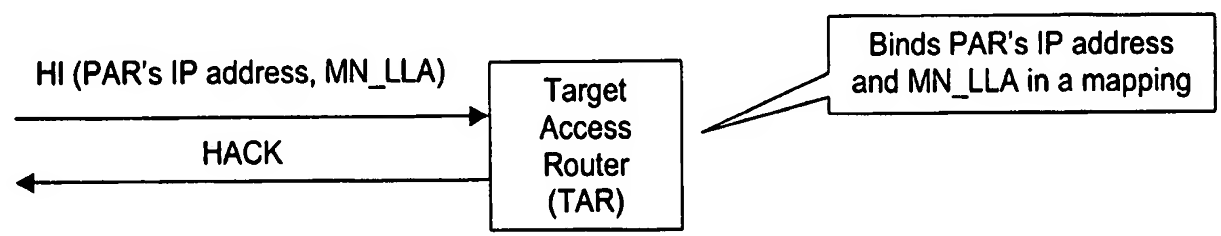

HI (PAR's IP address, MN_LLA)
HACK
Target Access Router (TAR)
Binds PAR's IP address and MN_LLA in a mapping

Fig. 4A

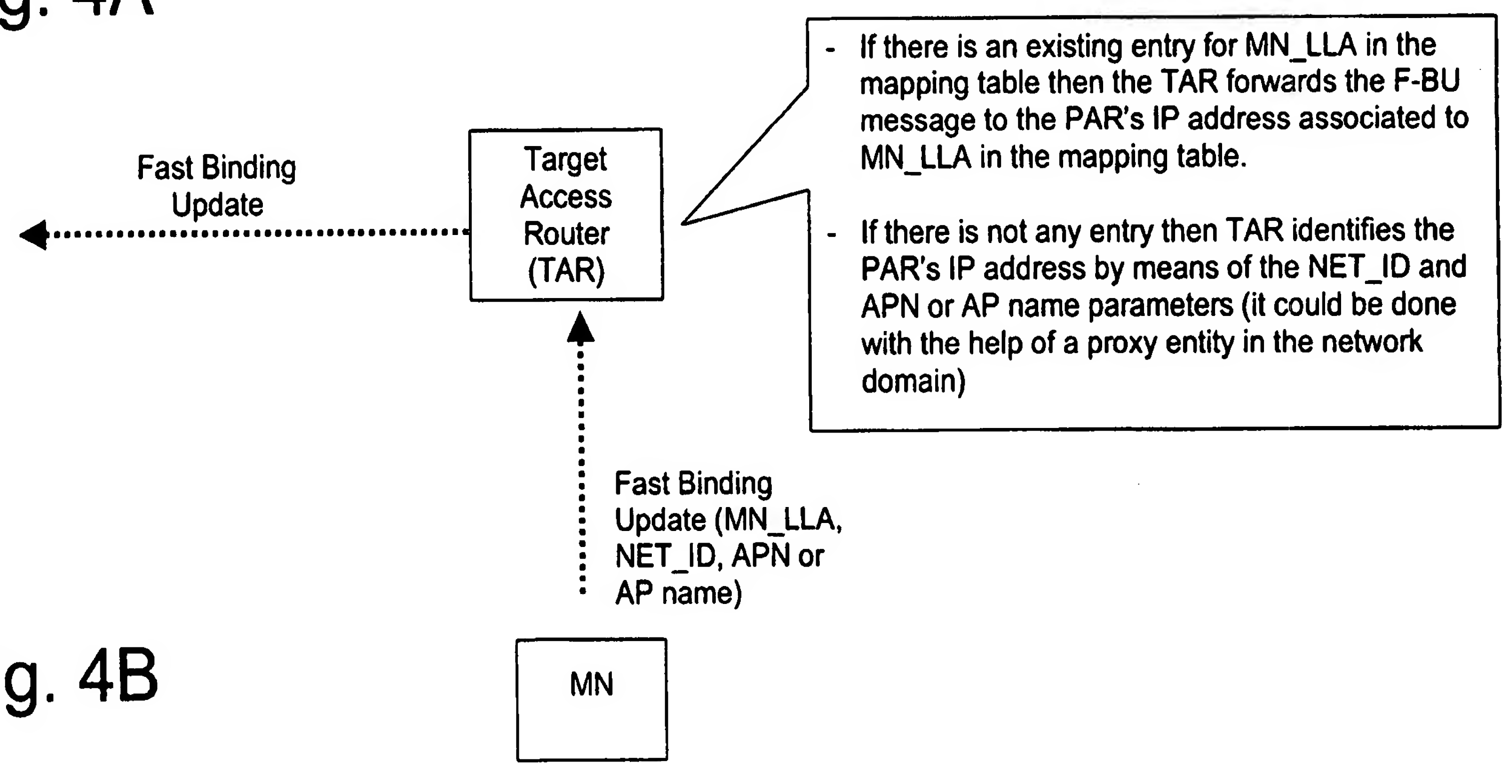

Fast Binding Update
Target Access Router (TAR)
- If there is an existing entry for MN_LLA in the mapping table then the TAR forwards the F-BU message to the PAR's IP address associated to MN_LLA in the mapping table.
- If there is not any entry then TAR identifies the PAR's IP address by means of the NET_ID and APN or AP name parameters (it could be done with the help of a proxy entity in the network domain)
Fast Binding Update (MN_LLA, NET_ID, APN or AP name)
MN

Fig. 4B

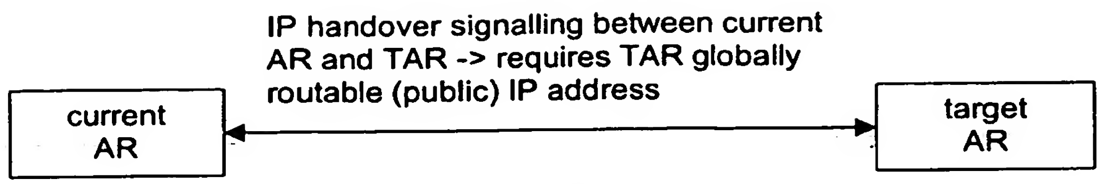

IP handover signalling between current
AR and TAR -> requires TAR globally
routable (public) IP address
current
AR
target
AR

Fig. 5

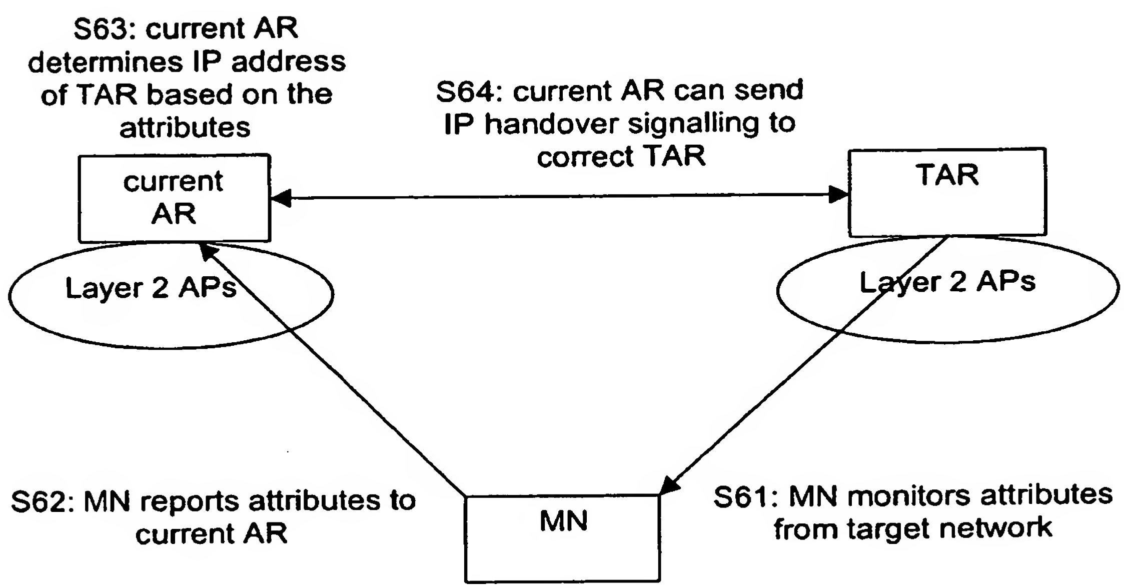

S63: current AR
determines IP address
of TAR based on the
attributes
S64: current AR can send
IP handover signalling to
correct TAR
current
AR
TAR
Layer 2 APs
Layer 2 APs
S62: MN reports attributes to
current AR
MN
S61: MN monitors attributes
from target network

Fig. 6

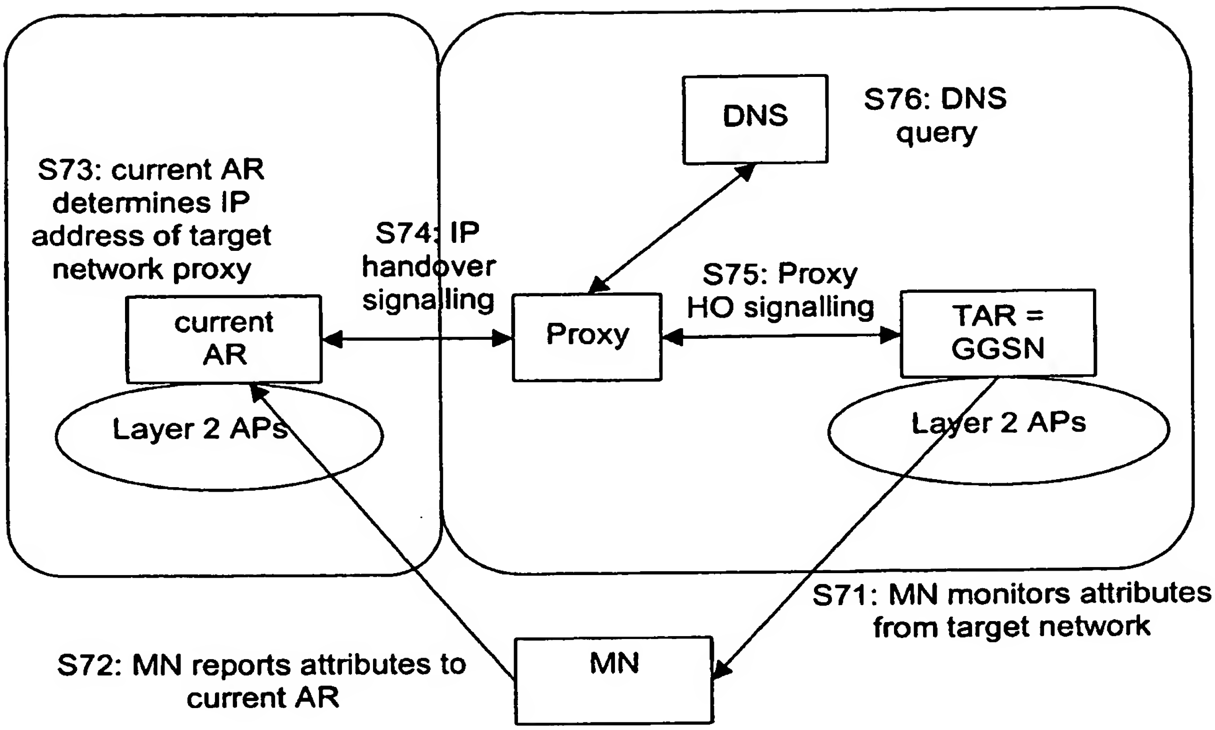
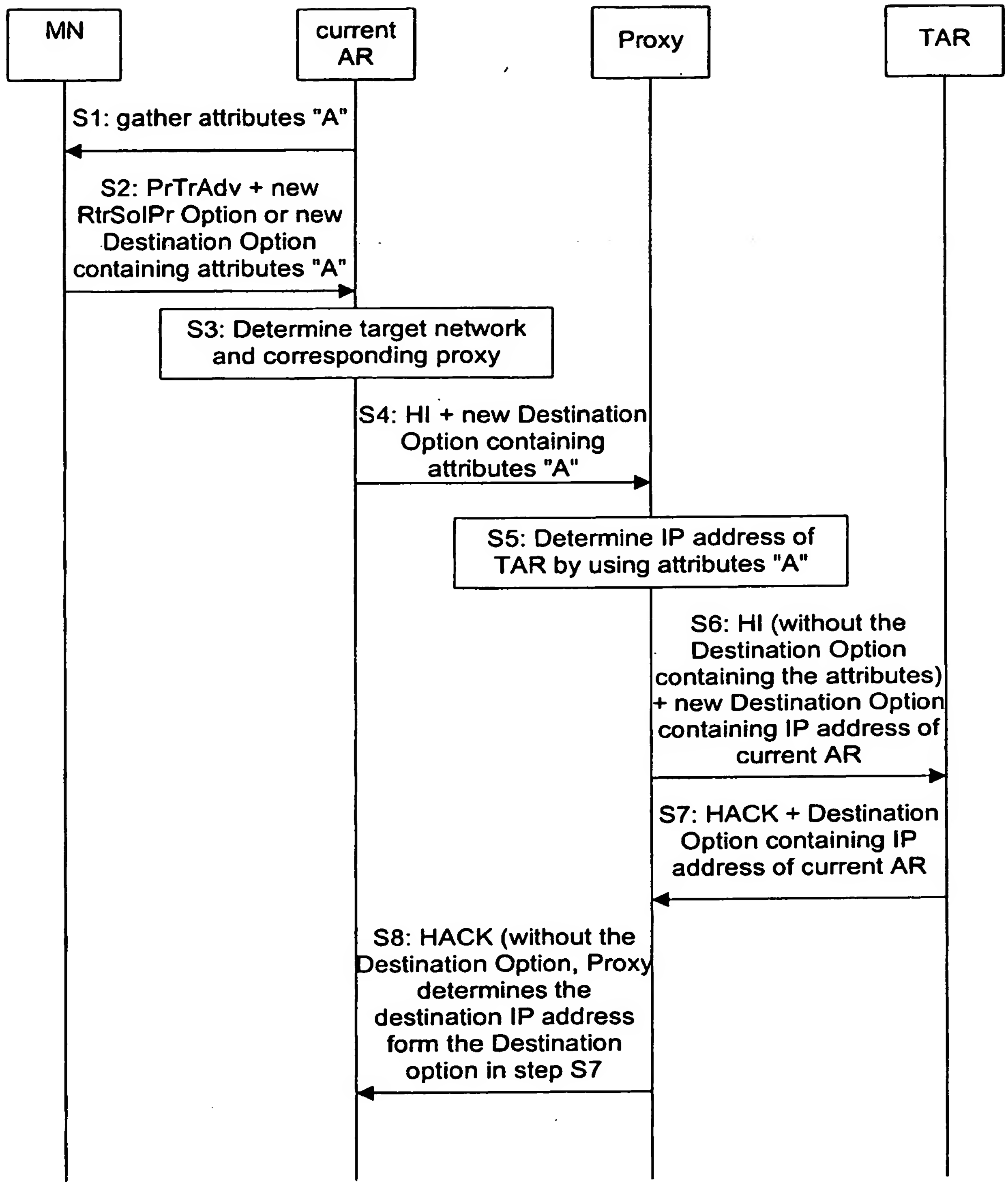

DNS
S76: DNS query
S73: current AR determines IP address of target network proxy
S74: IP handover signalling
S75: Proxy HO signalling
current AR
Proxy
TAR = GGSN
Layer 2 APs
Layer 2 APs
S71: MN monitors attributes from target network
S72: MN reports attributes to current AR
MN

Fig. 7



MN
current AR
Proxy
TAR
S1: gather attributes "A"
S2: PrTrAdv + new RtrSolPr Option or new Destination Option containing attributes "A"
S3: Determine target network and corresponding proxy
S4: HI + new Destination Option containing attributes "A"
S5: Determine IP address of TAR by using attributes "A"
S6: HI (without the Destination Option containing the attributes) + new Destination Option containing IP address of current AR
S7: HACK + Destination Option containing IP address of current AR
S8: HACK (without the Destination Option, Proxy determines the destination IP address form the Destination option in step S7

Fig. 8

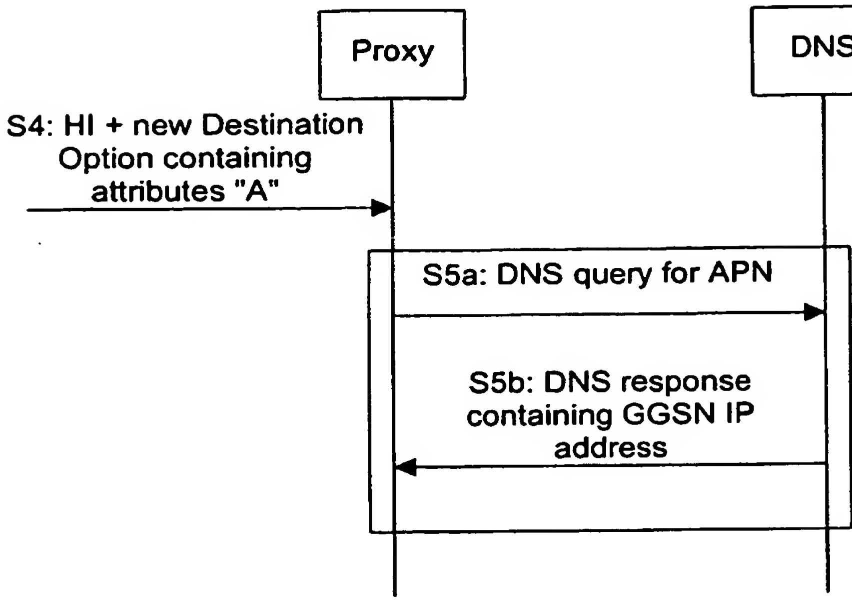

Proxy
DNS
S4: HI + new Destination Option containing attributes "A"
S5a: DNS query for APN
S5b: DNS response containing GGSN IP address

Fig. 9

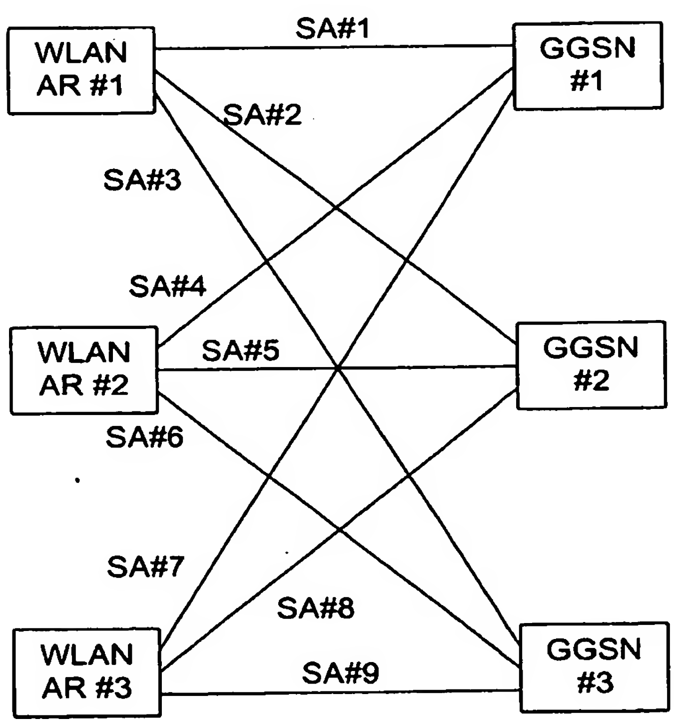

WLAN AR #1
WLAN AR #2
WLAN AR #3
GGSN #1
GGSN #2
GGSN #3
SA#1
SA#2
SA#3
SA#4
SA#5
SA#6
SA#7
SA#8
SA#9

Fig. 10

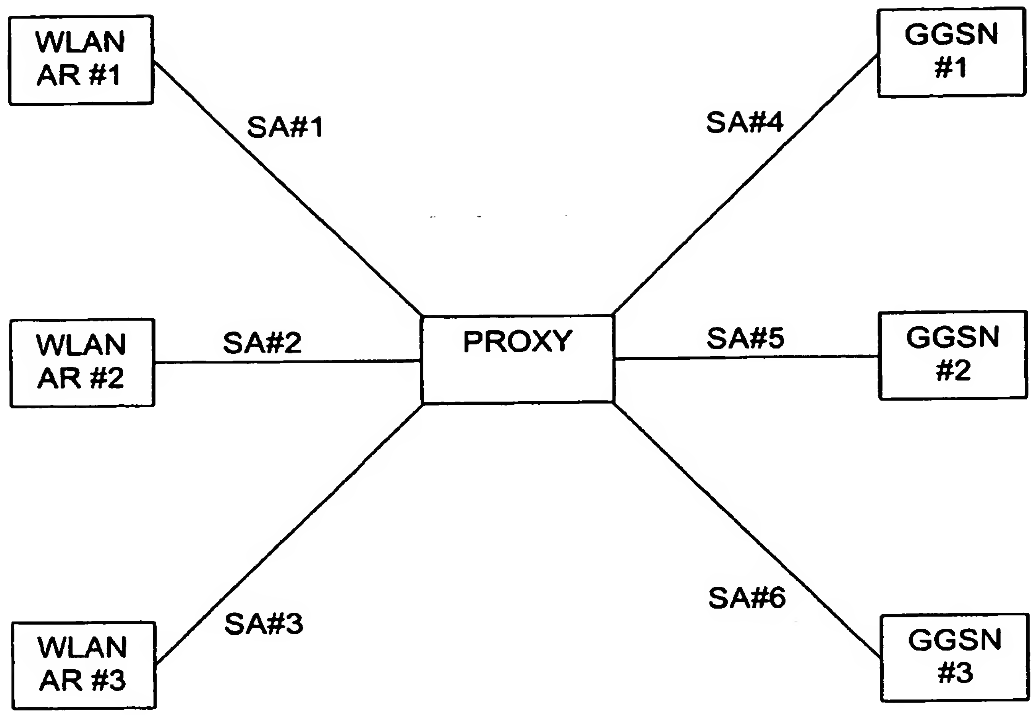

WLAN
AR #1
GGSN
#1
SA#1
SA#4
WLAN
AR #2
SA#2
PROXY
SA#5
GGSN
#2
SA#6
SA#3
WLAN
AR #3
GGSN
#3

Fig. 11

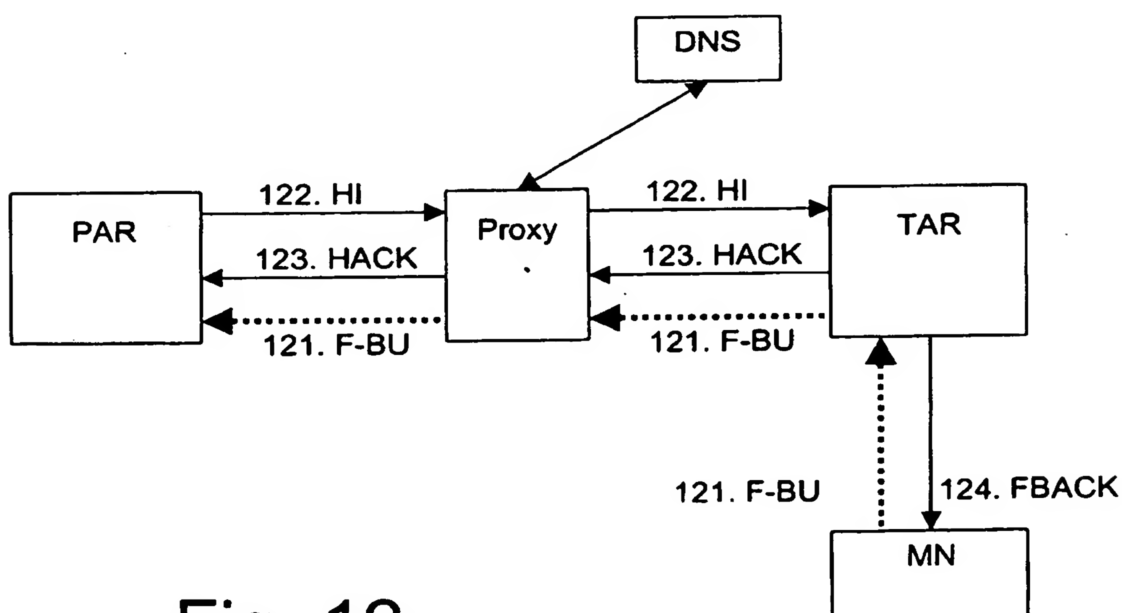

DNS
122. HI
122. HI
PAR
Proxy
TAR
123. HACK
123. HACK
121. F-BU
121. F-BU
121. F-BU
124. FBACK
MN

Fig. 12